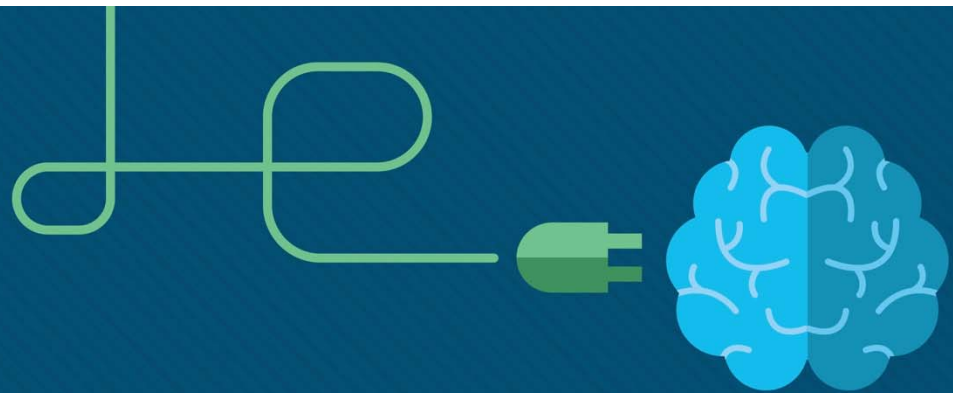


# Analiza e të dhënave të ndërrhyrjes



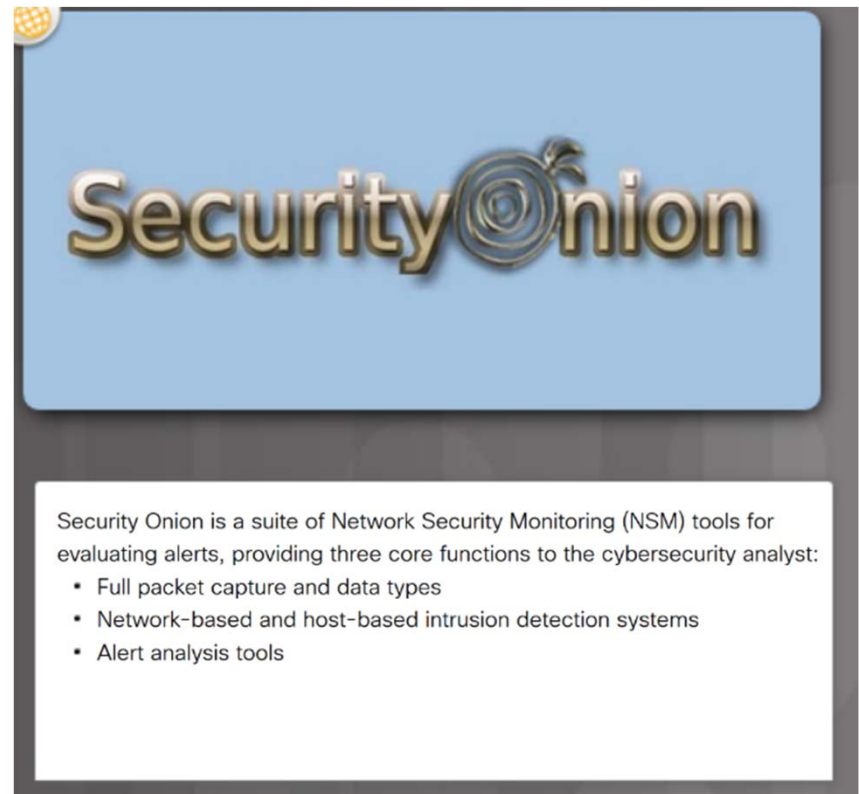
# Objektivat

- Vlerësimi i alarmeve
  - Shpjegoni procesin e vlerësimit të alarmeve.
    - Identifikoni strukturën e alarme.
    - Shpjegoni se si klasifikohen alarme.
- Duke punuar me të dhënat e sigurisë së rrjetit
  - Interpretimi i të dhënave për të përcaktuar burimin e një alarmi.
    - Shpjegoni se si janë përgatitur të dhënat për përdorim në një sistem të monitorimit të sigurisë së rrjetit (NSM).
    - Përdorni veglat e sigurisë së qepëve për të hetuar ngjarjet e sigurisë në rrjet.
    - Përshkruani veglat e monitorimit të rrjetit që rrisin menaxhimin e punës.
    - Mjekësia Ligjore Dixhitale
    - Shpjegoni se si analisti i sigurisë kibernetike merret me forenzikë dixhitale dhe dëshmi për të siguruar atributin e duhur të sulmit.
    - Shpjegoni rolin e proceseve digjitale mjeko-ligjore.

## Burimet e alarmeve

# Security Onion

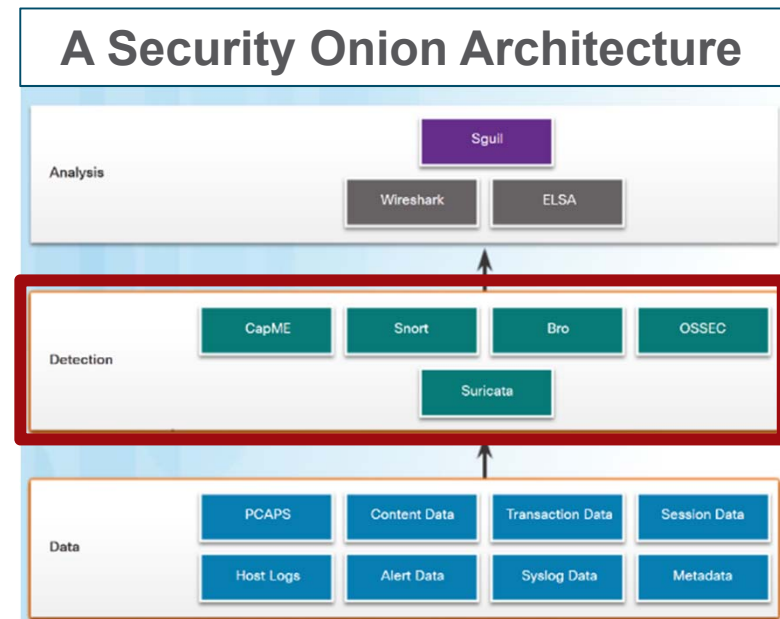
- Security Onion është një paketë me burim të hapur të mjeteve të Monitorimit të Sigurisë së Rrjetit (NSM) që funksionojnë në një shpërndarje të Ubuntu Linux.
- Disa nga komponentët e Security Onion janë në pronësi dhe mirëmbahen nga korporatat, si Cisco dhe Riverbend Technologies, por janë vënë në dispozicion si burim të hapur.



## Burimet e alarmeve

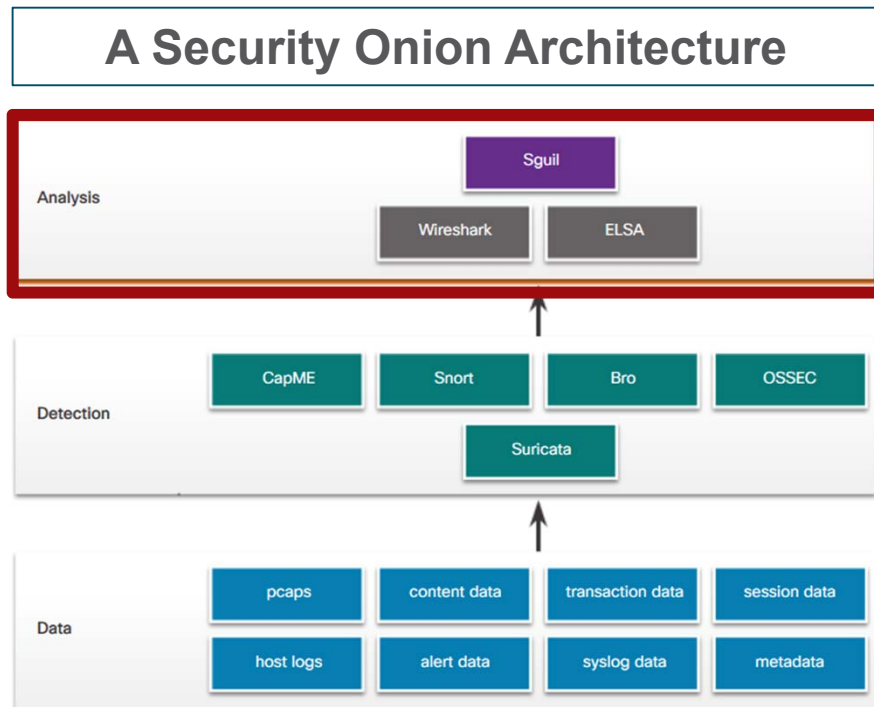
# Mjetet e zbulimit për mbledhje të të dhënave

- **CapME** siguron analistin e sigurisë kibernetike me një mjet të lehtë për t'u lexuar për të parë një sesion të tërë Layer 4.
- **Snort** përdor rregulla dhe nënshkrime për të gjeneruar alarme.
- **Bro** përdor politikat, në formën e skripteve që përcaktojnë se cilat të dhëna duhet të regjistrohen dhe kur duhet të lëshojnë njoftime njoftimi.
- **OSSEC** monitoron në mënyrë aktive operacionet e sistemit pritës, duke përfshirë kryerjen e monitorimit të integritetit të skedarëve, monitorimin e regjistrat lokal, monitorimin e proceseve të sistemit dhe zbulimin e rootkit.
- **Suricata** përdor multithreading amtare, i cili lejon shpërndarjen e përpunimit të transmetimit të pako-ve nëpër bërthama të procesorit të shumëfishta.



## Burimet e alarmeve

# Veglat për Analizim



- **Sguil** - Kjo siguron një konsol të nivelit të lartë të analistëve të sigurisë kibernetike për hetimin e alarme të sigurisë nga një shumëllojshmëri burimesh.
- **ELSA** - Burimet e regjistruara si HIDS, NIDS, firewalls, klientët syslog dhe serverat, shërbimet e domenit dhe të tjerët mund të konfigurohen për të bërë shkrimet e tyre në dispozicion për bazat e të dhënave ELSA.
- **Wireshark** - Ky është një aplikacion i kapjes së paketave që është integruar në suitë e Sigurisë së Qepave.

## Mjetet e analizës Gjenerimi i Alermeve

- Njoftimet janë të krijuara në Sigurinë e Qepës nga shumë burime, përfshirë Snort, Bro, Suricata, dhe OSSEC, ndër të tjera.
- Sguil siguron një tastierë që integron alarme nga burime të shumëfishta në një radhë me kohë të caktuar.
- Njoftimet në përgjithësi përfshijnë informacionin e mëposhtëm pesë-tuples:
  - SrcIP - adresa burimore e IP për ngjarjen.
  - SPort - burimi (lokal) Layer 4 për ngjarjen.
  - DstIP - IP destinacioni për ngjarjen.
  - DPort - destinacioni i shtresës 4 për ngjarjen.
  - Pr - numri i protokollit IP për ngjarjen.

## Sguil Window

The screenshot displays the Sguil Window interface, which is used for monitoring and analyzing network security alerts. The main window is divided into several sections:

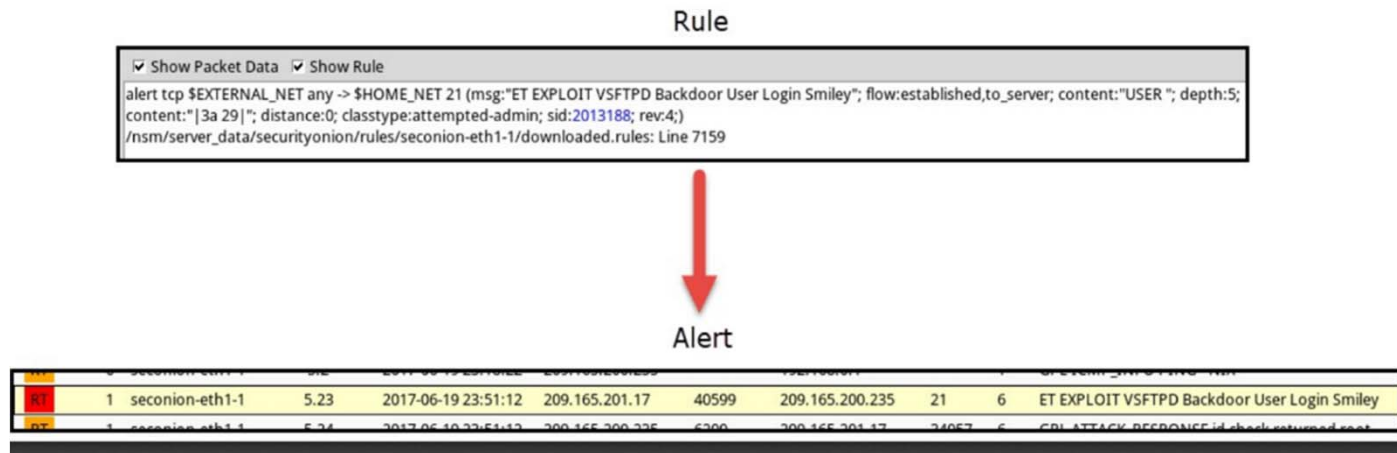
- Alerts List:** A table showing a list of alerts. Each row contains columns for ID, Host, Action, Alert ID, Date/Time, Src IP, Dst IP, Port, and Action. The alerts are sorted by Date/Time.
- Alert Details:** A section on the right side of the window showing the details of the selected alert. It includes a description of the alert, the source and destination IP addresses, the port, and the action taken.
- Alert Rules:** A section at the bottom of the window showing the rules that triggered the alert. It includes a list of rules and their corresponding actions.

The interface is designed to provide a comprehensive view of network security alerts, allowing users to quickly identify and respond to potential threats.

## Burimet e alarmeve

# Rregullat dhe Alarmet

- Alarmet mund të vijnë nga një numër burimesh:
  - NIDS - Snort, Bro dhe Suricata
  - HIDS - OSSEC
  - Menaxhimi dhe monitorimi i pasurive - Sistemi i Zbulimit të Aseteve Pasive (PADS)
  - Transaksionet HTTP, DNS, dhe TCP - Regjistruar nga Bro dhe pcaps
  - Mesazhet Syslog - Burime të shumëfishta



## Burimet e alarmeve

# Struktura e rregullave Snort

- Rregullat e gërhijve përbëhen nga rregullimet e rregullave dhe rregullat.
  - Kreu i rregullave përmban veprimin, protokollin, adresimin dhe informacionin e portit
  - Opsionet e rregullave përfshijnë mesazhin me tekst që identifikon alarmin edhe meta të dhënat në lidhje me alarmin.
- Rregullat e zbehta vijnë nga një shumëllojshmëri burimesh përfshirë kërcënimet në zhvillim (ET), SourceFire dhe Cisco Talos.
- PulledPork është një komponent i qepës së sigurisë që mund të shkarkojë rregullat e reja automatikisht nga snort.org.

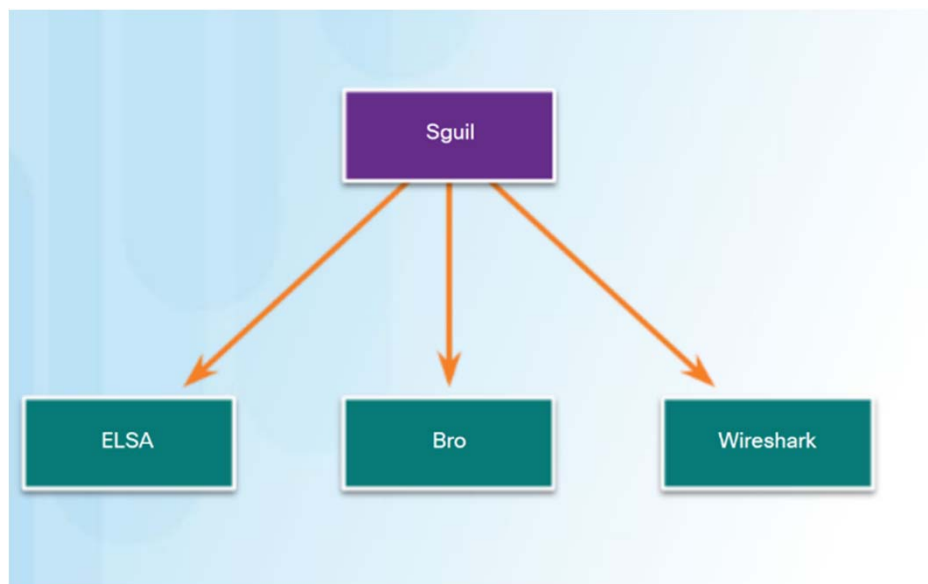
```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498;  
rev:8;)  
/nsm/server_data/securityonion/rules/seconion-eth1-1/downloaded.rules:Line 692
```

Component	Explanation
rule header	contains the action to be taken, source and destination addresses and ports, and the direction of traffic flow
rule options	includes the message to be displayed, details of packet content, alert type, source ID, and additional details, such as a reference for the rule or vulnerability
rule location	added by Sguil to indicate the location of the rule in the Security Onion file structure and in the specified rule file



## Vështrim i përgjithshëm i vlerësimit të paralajmërimit

### Nevoja për Vlerësimin e Alarmimit



- Shfrytëzimet në mënyrë të pashmangshme do t'i shmangen masave mbrojtëse, pavarësisht sa të sofistikuar mund të jenë.
- Rregullat e zbulimit duhet të jenë tepër konservatore.
- Është e nevojshme që analistët e kualifikuar të kibernetikës të hetojnë hetimet për të përcaktuar nëse një shfrytëzim ka ndodhur.
- Analizuesit e nivelit të parë të sigurisë kibernetike do të punojnë nëpërmjet rradhëve të alarme në një mjet si Sguil, duke u orientuar tek veglat si Bro, Wireshark dhe ELSA.

## Vështrim i përgjithshëm i vlerësimit të paralajmërimit

### Vlerësimi i alarmeve

- Alarmet mund të klasifikohen si më poshtë:
  - Vërtetë Pozitiv: Vigjilenca është verifikuar të jetë një incident i vërtetë sigurie.
  - False Pozitive: Vigjilimi nuk tregon një incident të vërtetë sigurie.
  - Negativ i vërtetë: Asnjë incident i sigurisë nuk ka ndodhur.
  - Negativ: Një incident i pazbuluar ka ndodhur.

When an alert is issued, it will receive one of four possible classifications		
	True	False
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred
Events classified as 'true' are desired.		

## Vështrim i përgjithshëm i vlerësimit të paralajmërimit

# Analiza Deterministe dhe Analiza Probabilistike

- Teknikat statistikore mund të përdoren për të vlerësuar rrezikun që shfrytëzon do të jetë i suksesshëm në një rrjet të caktuar.
  - Analiza Deterministe - vlerëson rrezikun bazuar në atë që dihet për një cenueshmëri.
  - Probabilistic Analysis - vlerëson suksesin e mundshëm të një shfrytëzimi duke vlerësuar mundësinë që nëse një hap në një shfrytëzim është përfunduar me sukses, hapi tjetër do të jetë i suksesshëm.

### Types of Analysis

---

- **Deterministic Analysis** - For an exploit to be successful, all prior steps in the exploit must also be successful. The cybersecurity analyst knows the steps for a successful exploit.
- **Probabilistic Analysis** - Statistical techniques predict the probability that an exploit will occur based on the likelihood that each step in the exploit will succeed.

# Puna me të dhënat e sigurisë së rrjetit

# Një platformë e përbashkët e të dhënave ELSA

The screenshot shows the ELSA web interface in a Chromium browser. The left sidebar contains a navigation menu with categories like Connections, Top / Status, and various protocols (DHCP, DNS, etc.). The main area displays a search query: `class=BRO_CONN " " proto="TCP"`. Below the query, there's a table of results with columns for Timestamp, Fields, and a detailed log entry. The table shows several records from June 19, 2017, at various times, detailing network connections and their associated data.

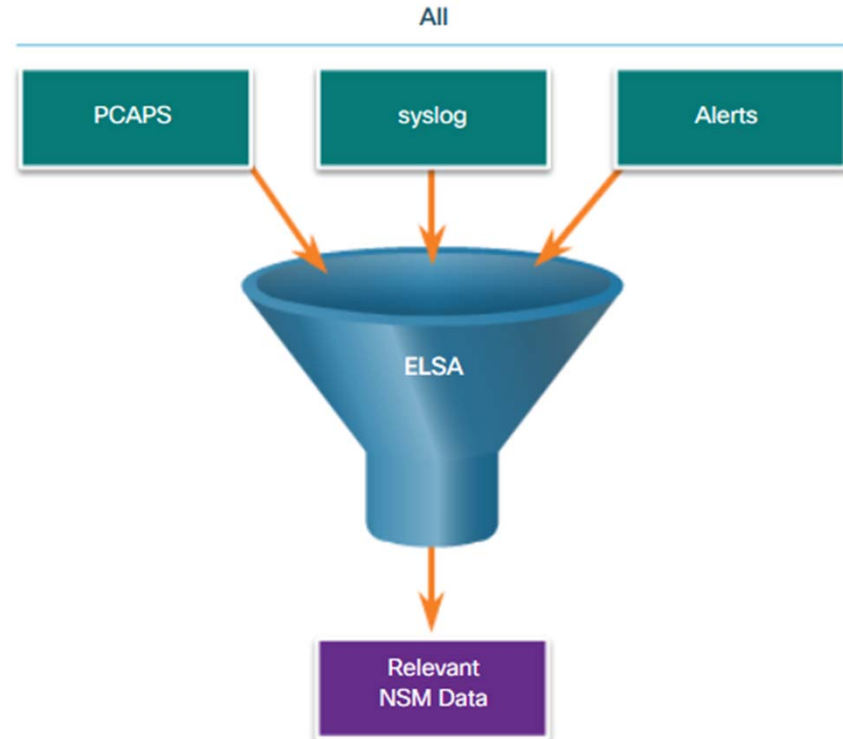
Timestamp	Fields	
Mon Jun 19 23:20:08	1497914398.753679/C6bJn43CDeE2YPwR1j209.165.201.17/40174/209.165.200.235/80tcp (3.027788)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info
Mon Jun 19 23:20:57	1497914495.813788/Cdn0W1WcCkxXjw209.165.201.17/40174/209.165.200.235/80tcp (3.027788)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info
Mon Jun 19 23:38:06	1497915471.544574/C6033X04BY112u3j209.165.201.17/40174/209.165.200.235/80tcp (3.040636)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info
Mon Jun 19 23:46:53	1497916001.850182/Cz0CAB15CnHGFgoT2g209.165.201.17/42642/209.165.200.235/443tcp (0.000367)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info
Mon Jun 19 23:46:53	1497916001.850182/Cz0CAB15CnHGFgoT2g209.165.201.17/42642/209.165.200.235/443tcp (0.000367)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info
Mon Jun 19 23:46:53	1497916001.850182/Cz0CAB15CnHGFgoT2g209.165.201.17/42642/209.165.200.235/443tcp (0.000367)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info
Mon Jun 19 23:51:20	1497916272.058095/CU4cev1qWyBjEeHC8j209.165.201.17/44235/209.165.200.235/6200tcp (0.000262)00050(TT)051180090 (empty)USUS\$seconion-eth1	Info
Mon Jun 19 23:51:28	1497916272.058095/CU4cev1qWyBjEeHC8j209.165.201.17/44235/209.165.200.235/6200tcp (0.000262)00050(TT)051180090 (empty)USUS\$seconion-eth1	Info
Mon Jun 19 23:53:10	1497916272.073566/CX9H93v7WvWk5Aryg209.165.201.17/4007/209.165.200.235/80tcp (3.027788)00050(TT)051180090 (empty)USUS\$seconion-eth2	Info

- Kërkesa dhe Arkivi i Regjistrimit të Ndërmarrjeve (ELSA) është një mjet i nivelit ndërmarrës për të kërkuar dhe arkivuar të dhënat e NSM që rrjedhin nga burime të shumta.
- ELSA është në gjendje të normalizojë shënimet e dosjeve të logaritjeve në një skemë të zakonshme që pastaj mund të shfaqet në ndërfaqen e internetit ELSA.
- ELSA merr shkrimet mbi Syslog-NG, regjistron dyqane në bazat e të dhënave MySQL, dhe indeksat duke përdorur Sphinx Search.

## Një platformë e përbashkët e të dhënave

### Reduktimi i te dhënave

- Reduktimi i të dhënave është identifikimi i të dhënave që duhet të grumbullohen dhe ruhen për të zvogëluar barrën e sistemeve.
- Duke kufizuar volumin e të dhënave, mjetet si ELSA do të jenë shumë më të dobishme.



## Një platformë e përbashkët e të dhënave

# Normalizimi i të dhënave

- Normalizimi i të dhënave është procesi i kombinimit të të dhënave nga një numër burimesh në një format të përbashkët për indeksimin dhe kërkimin.

Info	Mon Jun 19 23:46:27	1497915981.533031 Cgsy1R2aH21DCRtpa 209.165.201.17 51810 209.165.200.235 80 1 GET 209.165.200.235 /testmyids 1.1 curl/7.52.1 0 327 301 Moved Permanently -(empty) - FsjFMLpVbNYYitCdb text/html host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=209.165.201.17 srcport=51810 dstip=209.165.200.235 dstport=80 status_code=301 content_length=327 method=GET site=209.165.200.235 uri=/testmyids referer=- user_agent=curl/7.52.1 mime_type=text/html
Bro Log Format Fields	Normalized and Labelled ELSA Log Format Fields	
1497915981.533031	Mon Jun 19 23:46:27	
209.165.201.17 51810 209.165.200.235 80	srcip=209.165.201.17 srcport=51810 dstip=209.165.200.235 dstport=80	
327 301	status_code=301 content_length=327	
GET 209.165.200.235 /testmyids	method=GET site=209.165.200.235 uri=/testmyids	

## Një platformë e përbashkët e të dhënave

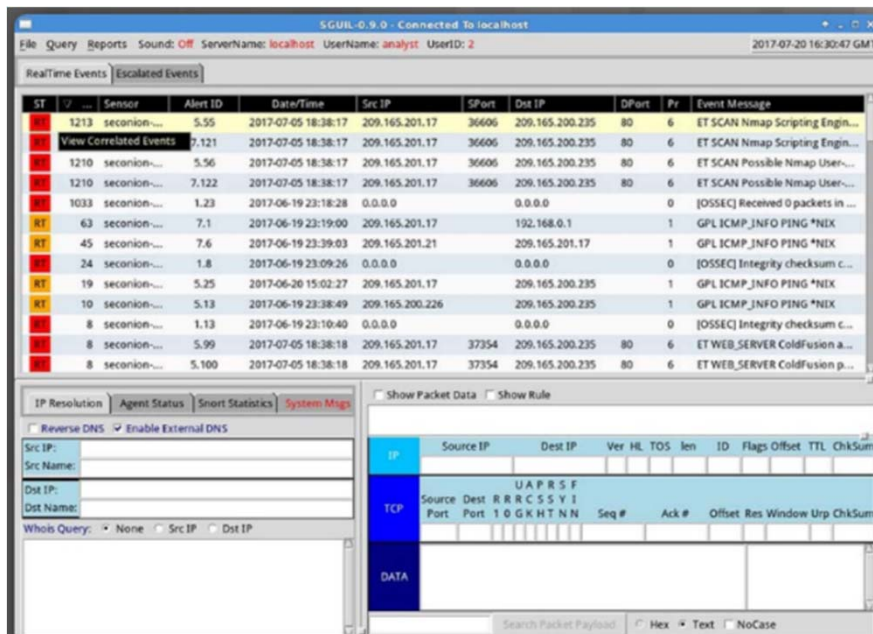
# Arkivimi i të dhënave



- Mbajtja e të dhënave NSM për një kohë të pacaktuar nuk është e mundshme për shkak të çështjeve të ruajtjes dhe qasjes.
- Korniza e pajtueshmërisë mund të kërkojë ruajtjen e të dhënave për një periudhë të caktuar kohe.
- ELSA mund të konfigurohet për të mbajtur të dhënat për një periudhë kohore. Parazgjedhja është 90 ditë.
- Të dhënat e alarmit të ruajtjes mbahen për 30 ditë me parazgjedhje.



## Hetimi i të dhënave të rrjetit Puna në Sguil



The screenshot shows the Sguil interface with a list of events and a packet analysis pane. The events list includes columns for ST, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The packet analysis pane shows details for a TCP packet, including Source IP, Dest IP, Ver, HL, TOS, Len, ID, Flags, Offset, TTL, ChkSum, and a search packet payload section.

ST	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	seconio...	5.55	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Nmap Scripting Engin...
RT	seconio...	5.56	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Possible Nmap User...
RT	seconio...	7.122	2017-07-05 18:38:17	209.165.201.17	36606	209.165.200.235	80	6	ET SCAN Possible Nmap User...
RT	seconio...	1.23	2017-06-19 23:18:28	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Received 0 packets in ...
RT	seconio...	7.1	2017-06-19 23:19:00	209.165.201.17	192.168.0.1	192.168.0.1	1	1	GPL ICMP_INFO PING *NEX
RT	seconio...	7.6	2017-06-19 23:39:03	209.165.201.21	209.165.201.17	209.165.201.17	1	1	GPL ICMP_INFO PING *NEX
RT	seconio...	1.8	2017-06-19 23:09:26	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integrity checksum c...
RT	seconio...	5.25	2017-06-20 15:02:27	209.165.201.17	209.165.200.235	209.165.200.235	1	1	GPL ICMP_INFO PING *NEX
RT	seconio...	5.13	2017-06-19 23:38:49	209.165.200.226	209.165.200.235	209.165.200.235	1	1	GPL ICMP_INFO PING *NEX
RT	seconio...	1.13	2017-06-19 23:10:40	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integrity checksum c...
RT	seconio...	5.99	2017-07-05 18:38:18	209.165.201.17	37354	209.165.200.235	80	6	ET WEB_SERVER ColdFusion a...
RT	seconio...	5.100	2017-07-05 18:38:18	209.165.201.17	37354	209.165.200.235	80	6	ET WEB_SERVER ColdFusion p...

- Në Security Onion, vendi i parë që një analist i sigurisë kibernetike do të shkojë për të verifikuar alarme është Sguil.
- Sguil korrespondon automatikisht alarme të ngjashme në një linjë të vetme dhe siguron një mënyrë për të parë ngjarjet e korreluara të përfaqësuara nga ajo linjë.

## Hetimi i të dhënave të rrjetit

# Sguil Queries

- Queries mund të ndërtohen në Sguil duke përdorur Query Builder, i cili thjeshton ndërtimin e pyetjeve.
- Analisti i sigurisë kibernetike duhet të njohë emrat e fushave dhe disa çështje me vlerat në terren.

The screenshot displays the Sguil interface, which is a network security monitoring tool. The top section shows a list of events with columns for ID, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The events listed are related to Nmap scanning and SQL injection attempts.

ID	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	seconion-eth1-1	5.521	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	seconion-eth1-1	5.522	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN NMAP SQL Spider Scan
1	seconion-eth1-1	5.523	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed
1	seconion-eth2-1	7.587	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
1	seconion-eth2-1	7.588	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN NMAP SQL Spider Scan
1	seconion-eth2-1	7.589	2017-07-05 18:38:29	209.165.201.17	40754	209.165.200.235	80	6	ET SCAN Possible Nmap User-Agent Observed

The bottom section shows a packet capture analysis for a specific event. It includes a table for packet details with columns for Source IP, Dest IP, Ver, HL, TOS, Len, ID, Flags, Offset, TTL, and ChkSum. The packet is identified as a GET request for a SQL injection payload.

Source IP	Dest IP	Ver	HL	TOS	Len	ID	Flags	Offset	TTL	ChkSum
209.165.201.17	209.165.200.235	4	5	0	268	33065	2	0	63	33914

The packet details section shows the following information:

- Source: 209.165.201.17
- Dest: 209.165.200.235
- Ver: 4
- HL: 5
- TOS: 0
- Len: 268
- ID: 33065
- Flags: 2
- Offset: 0
- TTL: 63
- ChkSum: 33914

The packet data section shows the following information:

- Source: 209.165.201.17
- Dest: 209.165.200.235
- Ver: 4
- HL: 5
- TOS: 0
- Len: 268
- ID: 33065
- Flags: 2
- Offset: 0
- TTL: 63
- ChkSum: 33914

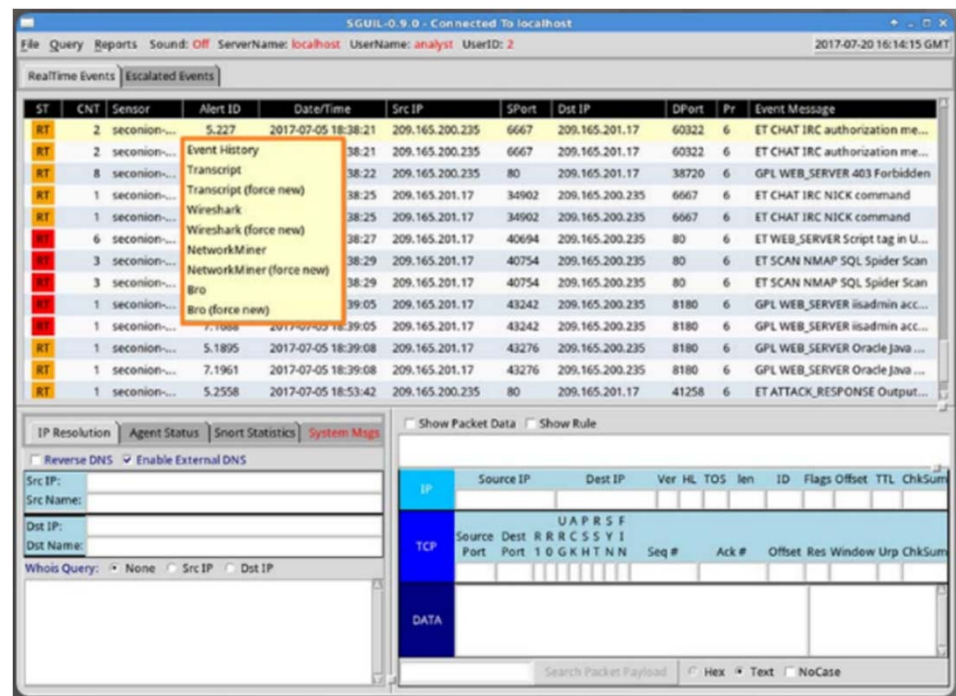
The packet data section shows the following information:

- Source: 209.165.201.17
- Dest: 209.165.200.235
- Ver: 4
- HL: 5
- TOS: 0
- Len: 268
- ID: 33065
- Flags: 2
- Offset: 0
- TTL: 63
- ChkSum: 33914

# Hetimi i të dhënave të rrjetit

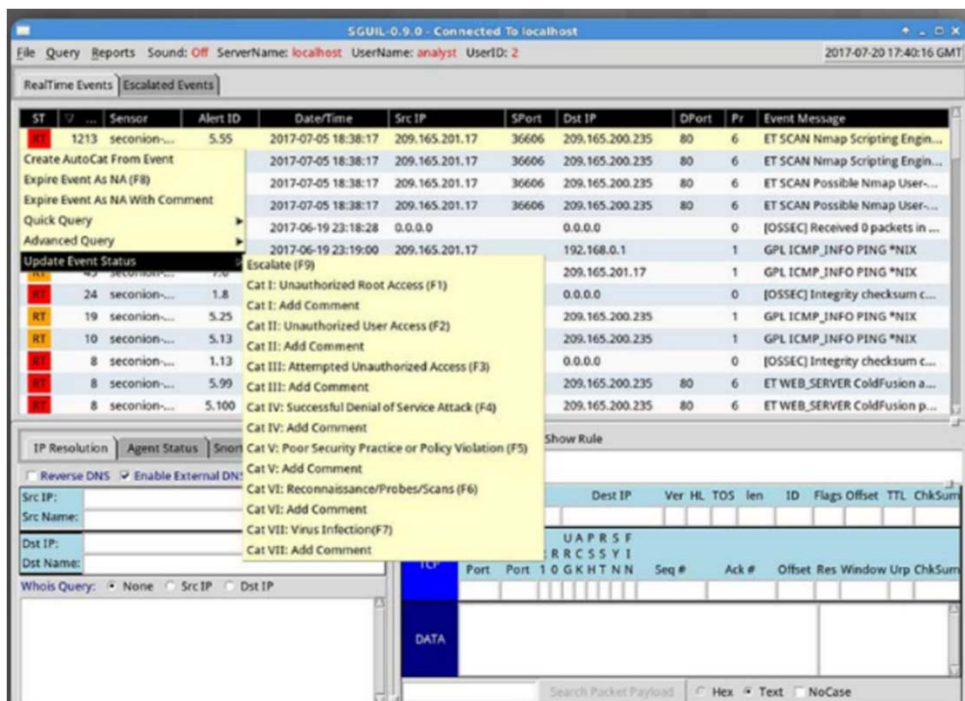
## Pivoting from Sguil

- Sguil siguron aftësinë për të "rrotulluar" hetimin në mjete të tjera të tilla si ELSA, Wireshark ose Bro.
- Log Files janë në dispozicion në ELSA, kapjet përkatëse të pakojeve mund të shfaqen në Wireshark, dhe transkriptet e sesioneve TCP dhe informacionet Bro janë gjithashtu në dispozicion.



## Hetimi i të dhënave të rrjetit

# Trajtimi i ngjarjeve in Sguil

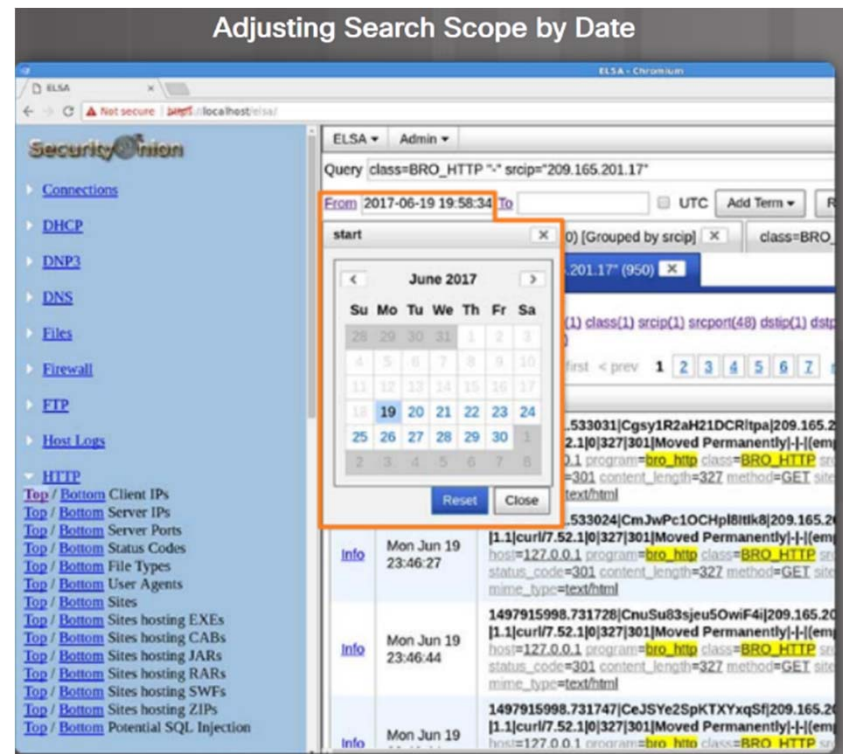


- Tre detyrat mund të kryhen në Sguil për të menaxhuar alarme.
- Alarmet që janë gjetur të jenë pozitive të rreme mund të skadojnë.
- Një ngjarje mund të përshkallëzohet duke shtypur butonin F9.
- Një ngjarje mund të kategorizohet.

## Hetimi i të dhënave të rrjetit

# Puna në ELSA

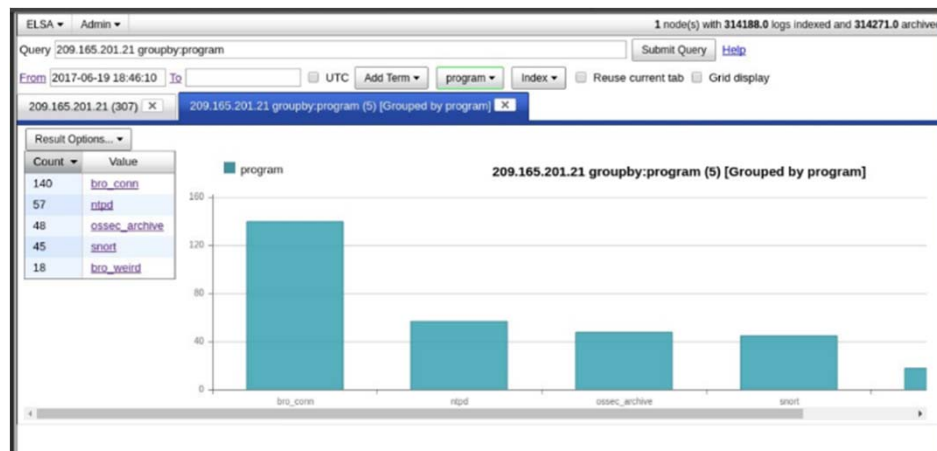
- ELSA siguron qasje në një numër të madh të shënimeve të dosjeve të logaritmeve.
- ELSA do të rifitojë vetëm 100 të dhënat e para për 48 orët e mëparshme.
- Mënyra më e lehtë për të parë informacionin në ELSA është lëshimi i pyetjeve të ndërtuara që shfaqen në të majtë të dritares ELSA dhe pastaj përshtatni datat dhe rifilloni pyetjen duke përdorur butonin Submit Query.



## Hetimi i të dhënave të rrjetit

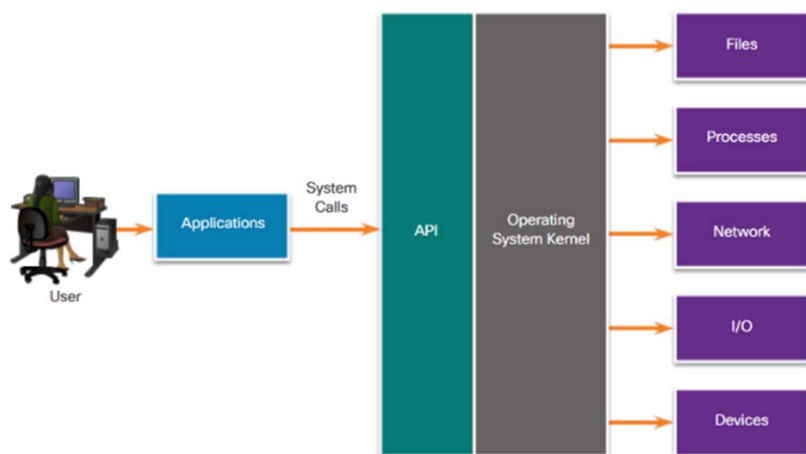
# Queries in ELSA

- ELSA ofron informacion në fushën e përmbledhjes dhe vlerës për çdo fushë që indeksohet në rezultatet e pyetjeve. Kjo lejon rafinimin e pyetjeve bazuar në një gamë të gjerë vlerash.
- Klikimi i një hyrjeje në kolonën e vlerës do të shfaqë pyetjen me vlerën e shtuar në pyetjen e mëparshme. Ky proces mund të përsëritet për të lehtësuar rezultatet e kërkimit me lehtësi.
- Shprehjet e rregullta ekzekutohen në ELSA duke përdorur funksionin grep.



Hetimi i të dhënave të rrjetit

## Procesi i Hetimit ose Thirrjet API



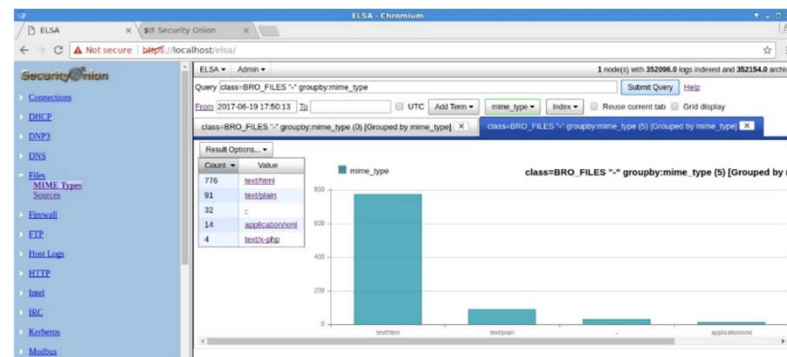
- Nëse malware mund të mashtrojë një kernel OS në lejin e saj për të bërë thirrje sistem, shumë shfrytëzime janë të mundshme.
- Rregullat OSSEC zbulojnë ndryshime në parametrat bazë të host-it, si ekzekutimi i proceseve softuerike, ndryshimet në privilegjet e përdoruesit dhe modifikimet e regjistrit, ndër të tjera.
- Rregullat e OSSEC do të shkaktojnë një alarm në Sguil.
- Zgjedhja e OSSEC si programi burimor në rezultatet e ELSA në një pamje të ngjarjeve OSSEC që ndodhën në host.



Hetimi i të dhënave të rrjetit

## Hetimi i detalizuar i të Dhënave

- Kur ELSA hapet drejtpërsëdrejti, ekziston një prerje e shkurtër e pyetjeve për skedarët.
- Hapja e pyetjeve të Dosjeve dhe zgjedhja e Llojave të Mimës në menynë shfaq një listë të llojeve të skedarëve që janë shkarkuar.
- Gjithashtu janë në dispozicion edhe skedarët MD5 dhe SHA-1 për skedarët e shkarkuar.
- Vlerat e hashave të skedarëve mund të dorëzohen në faqet në internet për të përcaktuar nëse skedari është i njohur me malware.





## Rritja e Punës së Analistit të Kibernetikës

# Dashboards dhe Vizualizimet

- Dashboards ofrojnë një kombinim interaktiv të të dhënave dhe vizualizimeve të dizajnuara për të përmirësuar vlerën e sasive të mëdha të informacionit.
- Lejoni analistët të përqëndrohen në detaje dhe informacione specifike
- ELSA i aftë të hartojë dashboards me porosi
- Squert ofron një ndërfaqe vizuale
- Cisco Talos ofron një pult kontrolli interaktive



## Rritja e Punës së Analistit të Kibernetikës

# Menaxhimi i fluksit të punës

- Monitorimi i sigurisë së rrjetit kërkon menaxhimin e flukseve të punës.
  - Përmirëson efikasitetin e ekipit të cyberoperations
  - Rrit përgjegjësinë e stafit
  - Siguron që të gjitha alarme të mundshme të trajtohen si duhet
  - Çdo alarm duhet të caktohet, përpunohet dhe dokumentohet sistematikisht
- Sguil siguron menaxhimin bazë të punës, por nuk është një zgjedhje e mirë për operacione të mëdha, sistemet e palës së tretë janë në dispozicion që mund të personalizohen
- Kërkesat e automatizuara shtojnë efikasitetin në rrjedhën e punës
  - Kërko për incidente komplekse të sigurisë që mund t'i shmangen mjeteve të tjera
  - Pyetja ELSA mund të konfigurohet si një rregull alarmi dhe të kryhet rregullisht
  - Mund të krijohet në një gjuhë të shkruar si Python